Competitiveness on Social Networking Sites and Its Implications on Individuals' Security and Privacy Concerns

Philip Menard
University of South Alabama
pmenard@southalabama.edu

Shwadhin Sharma
California State University, Monterey Bay
ssharma@csumb.edu

Abstract

Privacy and security of personal information in online settings continues to be a relevant and alarming issue for individuals who participate in social networking sites (SNS). A potential contributing factor of one's propensity to share information online could be level of competitiveness embedded in one's personality. Those who are more likely to socially engage in competitive activities may also be prone to conducting similar comparisons among peers in computer-mediated situations, such as SNS. In an effort to prove one's superiority in an online setting, one may unknowingly reveal important personal information. In this paper, we present a research model intended to help predict SNS usage based on users' innate propensity to be competitive with other SNS users, whether through the pure enjoyment of engaging in competition or via the desire to create conflict. Analysis of the model and potential implications are discussed further.

1. Introduction

Privacy and security of personal information in online settings continues to be a relevant and alarming issue for individuals who participate in social networking sites (SNS). Although the public's general awareness of these issues has increased in the last few years and led to more cautious behavior while online, a number of users have reported personally damaging consequences due to sharing information via social media, including identity theft, stalking and harassment, online scams, and hacked email accounts [1].

While many users have taken proactive measures toward protecting their online identities, there are others who may not be able to resist the urge to share personal information via SNS. A potential contributing factor of one's propensity to share information online could be level of competitiveness embedded in one's personality [2]. Those who are more likely to socially engage in competitive activities may also be prone to conducting similar comparisons among peers in computer-mediated situations, such as SNS. In an effort prove one's superiority in an online setting, one may unknowingly reveal important personal information.

The issues of information security and privacy may arise even further when a user is competing for attention in SNS. Several users of SNS engage in sharing of information to interact with other people and to attract their attention as well. However, in an information-rich context such as SNS, attention can be a scarce resource unless presented with interesting information about oneself. Thus, this study tries to understand how users' competitiveness affects their willingness to share information online.

This study is designed to answer the following research question: how does an individual's innate competitiveness affect his/her propensity to share information with peers in online settings?

2. Literature Review and Hypothesis Development

To better understand how SNS users may evaluate the cost-benefit analysis of determining whether to share information on the Internet, we have developed a conceptual research model that we will describe further in our study (see figure 1). We will first examine the formation of end users' concerns related to privacy in online settings and how this may influence one's decision to share information online via SNS.

2.1. Information Privacy Concerns

Internet privacy concerns are defined as individuals' perceptions of the consequences related to sharing information through the Internet [3]. Extant research has focused specifically on individuals' concerns with the information privacy practices of organizations [4]. A more general definition used by other researchers is an individual's personal views of fairness within the framework of information

URI: http://hdl.handle.net/10125/41761
ISBN: 978-0-9981331-0-2

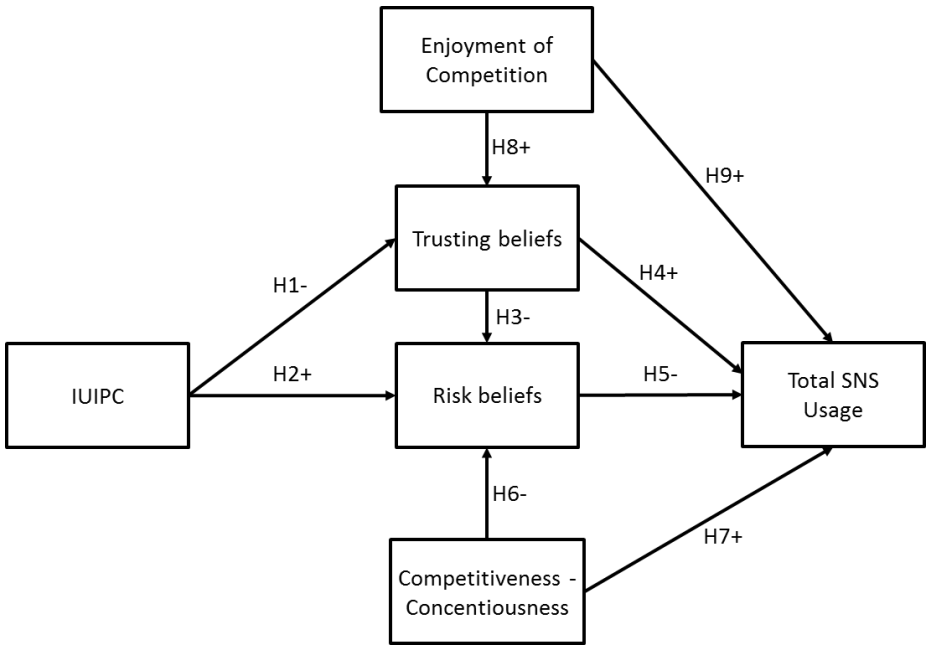

Figure 1: Conceptual model

privacy [5]. Previous research related to information privacy concerns has generally focused on explaining differences in levels of privacy concern by examining the influence of privacy concerns on a variety of dependent variables, including individuals' intention to participate in e-commerce or e-government transactions and disposition to share personal data with such organizations. Several studies have shown that individuals' intention to use online services are negatively influenced by information privacy concerns [6]–[9]. Information privacy concerns also have a negative effect on individuals' willingness to share personal data on the Internet [3], [6], [10]. Research has also shown that information privacy concerns affect individuals' attitudes related to the acceptance of technology [4], [5], [11].

Information privacy concerns are conceptualized in two widely accepted forms: concern for information privacy [4] and Internet user's information privacy concerns [5]. Concern for information privacy (CFIP) consists of four dimensions: collection of data, unauthorized secondary use of data, improper access to data, and errors in data. Alternatively, Internet user's information privacy concerns (IUIPC) is composed of three dimensions: control, awareness, and collection [5]. While CFIP is used by more researchers studying information privacy concerns, IUIPC has shown to explain more variance in its related dependent variables, such as willingness to share information online [12]. Because IUIPC is theoretically more parsimonious while providing more explanatory power, we will use this conceptualization of information privacy concerns in our study.

The interaction between IUIPC and behavioral intent is theoretically founded on the trust-risk framework [13] and the theory of reasoned action [14]. With regard to the trust-risk model, prior research focusing on information privacy has shown that trust and risk are the two most prominent individual beliefs which shape one's tendency to share personal information [15]–[17]. Trusting beliefs refer to the degree to which individuals believe an organization is reliable in guarding consumers' personal information [18], [19]. Risk beliefs are defined as perceptions that releasing personal information to an organization will expose the information to potential data loss or misuse [20]. Drawing from this framework, Malhotra et al. (2004) modeled IUIPC as having a positive effect on risk beliefs while negatively influencing trusting beliefs. Using the IUIPC model as a foundation, we provide the following hypotheses:

H1: SNS users' information privacy concerns will negatively influence trust beliefs.

H2: SNS users' information privacy concerns will positively influence risk beliefs.

H3: SNS users' trust beliefs will negatively influence risk beliefs.

The theory of reasoned action (TRA) states that behavioral intent is a consistent predictor of actual behavior [21]. Behavioral intent is used extensively in IS as a proxy for actual behavior when capturing actual behavior is unattainable or, as in many information security studies, the behavior in question is socially

undesirable. Previous studies have also shown trusting beliefs and risk beliefs to directly affect behavioral intent [13], [22]. The IUIPC model depicts trusting beliefs as positively affecting behavioral intent and risk beliefs as having a negative influence [5]. Based on TRA, we offer the following hypotheses:

H4: SNS users' trust beliefs will positively influence total SNS usage.

H5: SNS users' risk beliefs will negatively influence total SNS usage.

2.2. Competitiveness

Interaction on social networking sites provides a unique context for examining the privacy concerns of users that are not currently captured by the IUIPC framework. While sharing information online is typically related to receiving a greater level of convenience in return, sharing information on SNS environments could improve a user's social capital among those in his or her network. Social capital is a dynamic concept that is not only cultivated by a single person but requires the participation of multiple parties [2]. Because social capital requires the participation of at least two parties, human intimacy presents new challenges to consider.

Human beings have the habit of competing for attention, power, or attractiveness, especially when there are others who are also vying for it [23]. Be it the offline world (work, games, or school) or the online world (mobile games and social networks), competitions are ubiquitous. People compare themselves to others and compete for things for a variety of purposes. Social comparison theory explains that the tendency of people to self-evaluate by comparing themselves to others is an important source of competitive behavior (Garcia, Tor, and Schiff, 2013). Among the several dimensions of competitiveness, conflict and enjoyment of competition are often considered the primary dimensions that leads to competition [24].

Previous research studies have suggested that competitiveness is a multidimensional concept with users of SNS having different competitive attitudes towards social interaction and information sharing. Such competitive behaviors/traits are a part of a person's personality measure and can be of two types: enjoyment of competition and contentiousness [25], [26].

While some users in SNS environments may be concerned with establishing connections with other users, some may be more concerned with creating conflict among those in their networks. These users can be classified as having an increased innate desired to compete based on contentiousness – wanting to create conflict for the sake of proving one's superiority. These types of individuals are less prone to self-edit their words before stating them and are less risk averse in social interactions. Because one of the main goals this type of individual seeks is conflict and he/she regularly risks social capital by pursuing conflict, he/she is less likely to view an SNS environment as a risky outlet for sharing information. Because interacting on social networks satisfies an innate desire, a user who is driven by contentiousness will also demonstrate higher usage of social networks. Based on the preceding arguments, we present the following hypotheses:

H6: SNS users' competitiveness related to contentiousness will negatively influence risk beliefs.

H7: SNS users' competitiveness related to contentiousness will positively influence total SNS usage.

People who compete based purely on the enjoyment of competition offer an interesting counterpoint to those who behave in social interactions based on contentiousness. This type of person does not regularly risk social capital by exhibiting purposely contentious behavior. Rather, a person who enjoys competition will seek popularity through commonly shared beliefs in their social network (online or otherwise). For example, a person who enjoys competition will seek approval from their social network by sharing something relatable or desirable with their social network, like pictures of family or stories about a vacation, rather than garnering attention through conflict. While individuals who enjoy competition may still view some social interactions as risky (thus not having an effect on risk beliefs), they are more likely to trust their social network, as exhibited through their willingness to share personal (sometimes private) details to gain social capital. This behavior likely translates to SNS as well, with the enjoyment of competition leading to higher trusting beliefs related to an SNS. We offer the following hypothesis:

H8: SNS users' enjoyment of competition will positively influence trust beliefs.

Users engaging in social networks because of the enjoyment of competition want to be "liked", "popular", and "cool" on SNS. They express a positive attitude toward competition and present positive emotions and satisfaction during their interactions on SNS. Thus, the increased sharing of information may also be attributed to a person's innate desire to compete with others purely for the enjoyment of competition. The increase in social capital is apparent to users when connections are made in social networks. Some users may subconsciously become more fixated on the

amount of social capital gained in comparison to their peers in SNS. This could potentially lead to end users conducting online interactions with no regard toward the type of information that is required to share to gain additional social capital. We offer the following hypotheses:

H8: SNS users' enjoyment of competition will positively influence trust beliefs.

H9: SNS users' enjoyment of competition will positively influence total SNS usage.

3. Methods

To thoroughly examine users' competitiveness in the context of SNS, we have developed an instrument for assessing SNS users' inherent levels of competitiveness, privacy concerns related to the Internet, and their overall volume of SNS usage. This section provides a detailed description of the measurement scales used and the tools used for analysis.

3.1. Measures and Instrumentation

Respondents were first presented with items to determine their SNS membership. The respondents had the choice to select their SNS membership from the list of 15 most popular social network sites based on total membership. Respondents were asked to check each social network where they are a current member. By including a text box below the list of SNS, we also gave respondents the option to report their membership to other SNS not included in the list. For each SNS the respondent reported as being a current member, they were asked to report the frequency with which they post information on that particular SNS. If the respondent reported that he posted information daily, he was then asked to report the approximate number of times per day he posts information to the SNS. A respondent's total SNS usage was calculated to represent his approximate number of posts across all SNS for a given month.

After respondents were iterated through each of their SNS memberships for frequency reporting, the respondents were also assessed on perceptions of information privacy concerns, trusting beliefs, risk beliefs, and competitiveness. This study also calculated general demographics questions such as age, gender, computer experience, education level, prior experience with personal privacy invasions, and exposure to news related to information privacy violations.

The following latent constructs were measured with multi-item scales: information privacy concerns, trusting beliefs, risk beliefs, and competitiveness to adopt smart metering technology. Scales for trusting beliefs and risk beliefs were adapted from Jarvenpaa, et al. [22]. Scales for each of the IUIPC dimensions (collection, control, and awareness) were adapted from Malhotra, et al. [5]. Scales for competitive enjoyment and contentiousness were adapted from Harris and Houston [27]. Each item was measured using a five-point Likert scale, and all items were fully anchored from "strongly disagree" to "strongly agree."

3.2. Common Method Bias

When collecting data using a single method, common method bias may become a potential problem. Because we are using self-report 5-point Likert scales to collect our data, the present study may be susceptible to common method bias. As such, we followed guidelines for minimizing common method bias [28]. We randomized the items within the instrument to mitigate order effect. We reduced the impact of social desirability bias by ensuring respondent anonymity. We conducted post-hoc analyses to identify response set or unreasonably short survey completion times.

3.3. Panel and Pilot Testing

Following the initial design of our instrument, we conducted an expert review panel, which consisted of subject matter experts and experts in survey instrument design. The panel was largely comprised of faculty and doctoral students with quantitative analysis and research design experience. Subsequently, we administered a pilot study to assess convergent and discriminant validity of our scales. The pilot study showed factor loadings that meets accepted thresholds and confirmed the validity of our scales and led to no change in the instrument design.

3.4. Participants

To confirm validity of the sampling frame, we used filter questions as survey openers to ensure that the respondents for this survey are a current SNS account holders. We chose this sample to capture the true perceptions of actual SNS users who often make decisions regarding the sharing of information on the SNS. 250 respondents were solicited to participate in the survey through Amazon Mechanical Turk. After eliminating responses due to incomplete response set, unreasonably short completion times, and/or failed manipulation checks, we retained 202 usable responses.

Table 1: Loadings and cross-loadings

	CC	CE	RB	TB	Composite Reliability
CC1	.824	-.069	-.230	-.066	.820
CC2	.744	-.118	-.152	-.261	
CC3	.761	-.117	-.246	.033	
CE1	-.090	.836	.001	-.274	.950
CE2	-.043	.814	-.028	-.162	
CE3	-.162	.843	.081	-.169	
CE4	-.146	.861	.024	-.183	
CE5	-.113	.809	-.004	-.291	
CE6	-.076	.797	.007	-.235	
CE7	-.140	.865	.067	-.244	
CE8	-.127	.848	.009	-.234	
CE9	-.053	.719	.102	-.203	
RISK1	-.223	.006	.820	-.142	.874
RISK2	-.260	-.001	.701	.076	
RISK3	-.218	.083	.793	.123	
RISK4	-.258	.037	.741	.036	
RISK5	-.069	.017	.754	.014	
TRUST1	-.132	-.290	-.021	.750	.897
TRUST2	-.143	-.186	-.079	.830	
TRUST3	-.045	-.230	-.034	.891	
TRUST5	-.047	-.247	.014	.791	

Table 2: AVE and shared variance of latent constructs

	AVE	CC	CE	Risk	Trust
CC	.604	(.777)			
CE	.678	-.128	(.823)		
Risk	.582	-.277	.033	(.763)	
Trust	.685	-.109	-.297	-.036	(.828)

( ) = square root of AVE

Table 3: Hypothesis support

Hypothesis (with Direction)	Path Coefficient	T-Statistic	P-Value	Supported?
H1: IUIPC → TB	-0.108	0.911	p > .05	Not Supported
H2: IUIPC → RB	0.575	9.618	p < .001	Supported
H3: TB → RB	-0.004	0.060	p > .05	Not Supported
H4: TB → SNS Usage	0.159	2.755	p < .01	Supported
H5: RB → SNS Usage	-0.021	0.301	p > .05	Not Supported
H6: CC → RB	-0.210	3.219	p < .01	Supported
H7: CC → SNS Usage	-0.046	0.579	p > .05	Not Supported
H8: CE → TB	0.301	4.281	p < .01	Supported
H9: CE → SNS Usage	0.115	2.057	p < .05	Supported

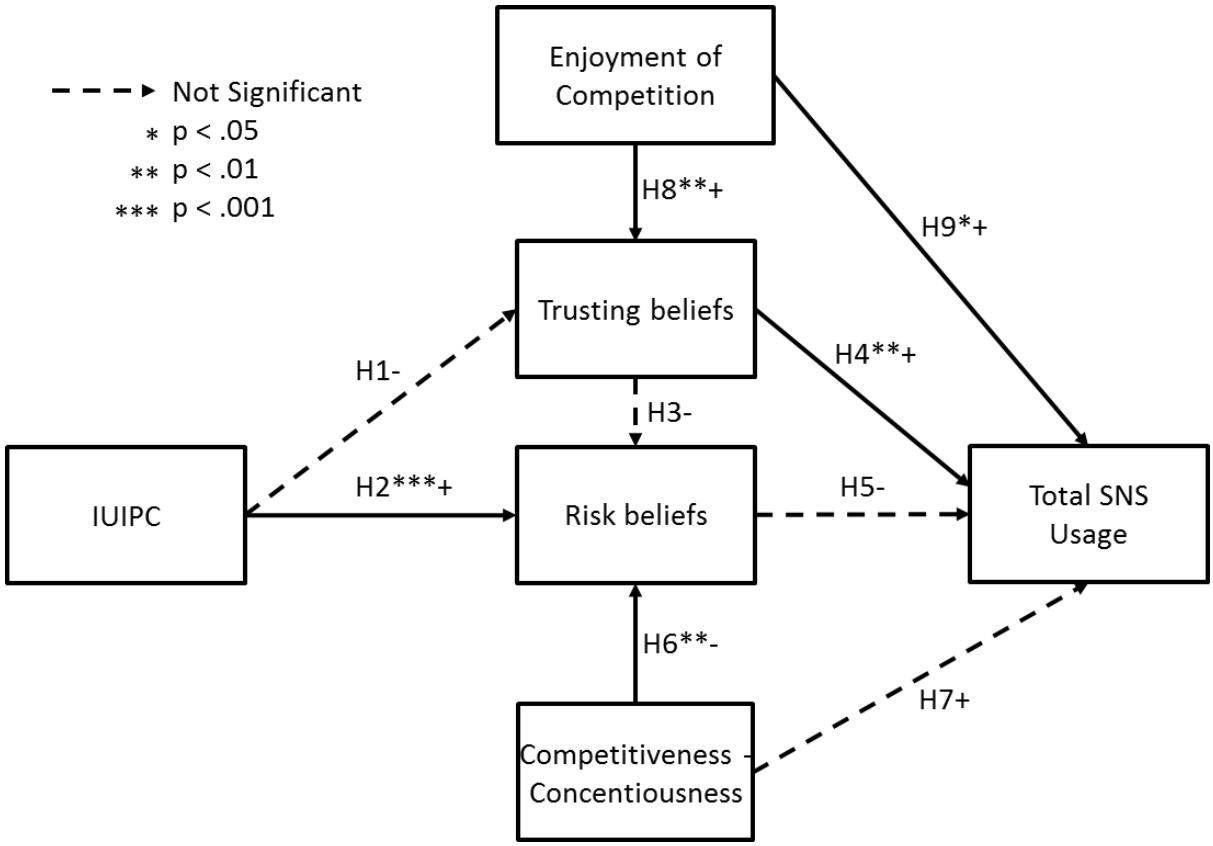

Figure 2: Results of structural model analysis

4. Data Analysis and Results

This portion of the study explains the data analysis techniques used, including descriptions of instrument validity assessment, construct validity tests, and analysis of the conceptual model. Results are further illustrated in model and tabular presentations.

4.1. Instrument Validity

Because risk beliefs, trust beliefs, and competitiveness were conceptualized as reflective, multi-item scales were used to measure these constructs. To ensure consistency among items within a scale, adequate reliability must be demonstrated. Composite reliability was calculated for each reflective scale. Reliability exceeded 0.8 for each scale, showing sufficient consistency among each scale's items [29]–[31]. Convergent validity is established to ensure each item measuring a particular construct is significantly correlated with its construct's composite value [32]. Examining partial least squares (PLS) reports for cross-loadings, convergent validity was significantly established for all constructs. Discriminant validity was also demonstrated when measuring constructs reflectively. Cross-loadings between all constructs were not significant. Table 1 illustrates loadings and cross-loadings, as well as composite reliability, for all reflective scale items. Convergent and discriminant validity were also examined by comparing shared variance between constructs with the average variance extracted (AVE) of the respective constructs [33]. AVE for each construct should exceed .5, and shared variance between constructs should not exceed either of the constructs' AVEs. Although some cross-loading was evident between constructs, each construct's AVE exceeded .5 and was greater than any variance shared with other constructs. Shared variance and AVEs for each construct is depicted in Table 2.

4.2. PLS Analysis

Our structural model and its associated hypotheses were tested using SmartPLS [34]. In addition, a bootstrapping resampling technique, which approximates the path coefficients and the amount of variance explained in mediating variables was used.

H2, H4, H6, H8, and H9 were supported, while the remaining hypotheses were not found to be significant. Our overall findings for hypotheses support are shown in Table 3. As illustrated in Figure 4, the model explains approximately 4 percent of the variance in total SNS usage, demonstrating that support for the research model is quite limited [35]–[37]. Insights yielded from the data are discussed below.

Some of the hypothesized relationships were well-supported, while others were not. Each of the significant hypotheses was supported at an alpha level of .05 or lower. Consistent with the hypothesized relationships, information privacy concerns had a significant positive effect on risk beliefs ($\beta = .575$, $p < .001$) but did not have a significant positive relationship with trust beliefs ($\beta = -.108$, $p > .05$). Trust beliefs did not negatively influence risk beliefs ($\beta = -.004$, $p > .05$) but had a significant positive effect on total SNS usage ($\beta = .159$, $p < .01$). Risk beliefs did not have a significant negative influence on total SNS usage ($\beta = -.021$, $p > .05$). Competitiveness related to contentiousness had a significant positive effect on risk beliefs ($\beta = .210$, $p < .01$) but did not have a significant effect on total SNS usage ($\beta = -.046$, $p > .05$). Competitiveness related to the enjoyment of competition had a significant positive effect on trust beliefs ($\beta = .301$, $p < .01$) and a significant positive effect on total SNS usage ($\beta = .115$, $p < .05$).

We conducted additional analyses to determine the impact of various demographic variables. None of the included demographics (age, gender, computer experience, education level, prior experience with personal privacy invasions, and exposure to news related to information privacy violations) had a significant impact on total SNS usage. However, computer experience demonstrated a significant negative effect on both trusting beliefs ($\beta = -.198$, $t = 2.811$, $p < .01$) and risk beliefs ($\beta = -.128$, $t = 2.015$, $p < .05$).

5. Discussion

5.1 Overall Findings

The IUIPC model seems to only be partially supported in the context of SNS usage, as our data shows that there is a break in the some of the IUIPC model's typically supported relationships. First, IUIPC did not affect trusting beliefs. This finding shows that for SNS contexts, even though users may have concerns related to the privacy of their information, users' trust in SNS does not waver. This could be due to the implicit understanding that users have about SNS prior to interacting on them; for SNS to provide its purported utility, users must share information.

IUIPC significantly influenced risk beliefs, but risk beliefs did not affect total SNS usage. Similarly, competitiveness related to contentiousness significantly affected risk beliefs but did not have an impact on total usage. Again, this finding may be due to users' implicit understanding of the risks associated with participating in SNS. Although our hypothesis of contentious SNS users being less risk averse and having lower perceptions of risk beliefs was supported, users simply evaluate their perceptions of the risks as being not significant enough to disengage from social networks.

Trusting beliefs demonstrated a positive effect on total SNS usage, showing that trust matters to users when they make the decision to engage with the SNS by sharing information. This finding shows that while users are implicitly aware of the privacy concerns and risk beliefs associated with using social networks, users who trust their social network will contribute and share more information. Interestingly, trusting beliefs did not affect risk beliefs.

The enjoyment of competitiveness demonstrated significant influence when included in the IUIPC model, specifically affecting both trust beliefs and total SNS usage. This could possibly indicate that end users who possess an innate enjoyment of engaging in competitive activities may also experience an inflated sense of trust in a SNS due to its ability to satiate a competitive desire. This is also reflected in the significant positive effect the enjoyment of competition has on total SNS usage, demonstrating that those who enjoy competition significantly increase their sharing on SNS environments. The need for gaining social capital in relation to other SNS users is a significant factor in this context and offers interesting theoretical implications, discussed further in the next section.

5.2 Implications on Theory

Our findings provide interesting insights in the application of the IUIPC model in online contexts that differ from typical e-commerce transactions. Online social networks are fundamentally different in that user interactions, transactions of social capital, and implicit comparisons between users regularly occur. With the utility of SNS being completely reliant on the sharing of information from users, the significance of IUIPC's foundational variables (privacy concerns, trusting beliefs, risk beliefs) is impacted. Our findings also demonstrate that other factors, such as competitiveness, can significantly influence IUIPC's foundational variables. Our research, while exploratory in nature, may provide an important building block in

developing alternative models to better explain users' evaluation of security and privacy while engaging in SNS.

While the enjoyment of competition did provide a significant positive influence on the IUIPC model, the amount of variance in total SNS usage that was explained by the model was quite low. This indicates that other constructs not measured in the present study will likely offer better explanatory power toward predicted user sharing behavior on SNS. Although the contribution of the present study is limited, the results demonstrate that there are interesting research opportunities to further explore the phenomenon at hand to discover the underlying factors that significantly contribute to users sharing information on SNS environments.

6. Conclusion

Although SNS has provided users with a convenient way to stay connected with one another, it remains an attractive threat vector for hackers to potentially find susceptible victims. By understanding why some users may share too much information, researchers may be able to construct appeals to warn users about the risks associated with revealing too much in online settings.

7. References

[1] L. Rainie, A. Smith, and M. Duggan, "Coming and going on Facebook," *Pew Research Center's Internet and American Life Project*, 2013.

[2] R. S. Burt, "The Social Structure of Competition," *Explor. Econ. Sociol.*, vol. 65, pp. 57–91, 1993.

[3] T. Dinev and P. Hart, "An Extended Privacy Calculus Model for E-Commerce Transactions," *Inf. Syst. Res.*, vol. 17, no. 1, pp. 61–80, Mar. 2006.

[4] H. J. Smith, S. J. Milberg, and S. J. Burke, "Information Privacy: Measuring Individuals' Concerns About Organizational," *MIS Q.*, vol. 20, no. 2, pp. 167–196, 1996.

[5] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Inf. Syst. Res.*, vol. 15, no. 4, pp. 336–355, Dec. 2004.

[6] F. Bélanger, J. Hiller, and W. J. Smith, "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes," *J. Strateg. Inf. Syst.*, vol. 11, no. 3/4, pp. 245–270, 2002.

[7] R. K. Chellappa and R. G. Sin, "Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Inf. Technol. Manag.*, no. 6, pp. 181–202, 2005.

[8] M. A. Eastlick, S. L. Lotz, and P. Warrington, "Understanding Online B-to-C Relationships: An Integrated Model of Privacy Concerns, Trust, and Commitment," *J. Bus. Res.*, vol. 59, no. 8, pp. 877–886, 2006.

[9] M. L. Resnick and R. Montania, "Perceptions of Customer Service, Information Privacy, and Product Quality From Semiotic Design Features in an Online Web Store," *Int. J. Hum. Comput. Interact.*, vol. 16, no. 2, pp. 211–234, 2003.

[10] D. L. Hoffman, T. P. Novak, and M. Peralta, "Building Consumer Trust Online," *Commun. ACM*, vol. 42, no. 4, pp. 80–85, 1999.

[11] K. A. Stewart and A. H. Segars, "An Empirical Examination of the Concern for Information Privacy Instrument," *Inf. Syst. Res.*, vol. 13, no. 1, pp. 36–49, Mar. 2002.

[12] F. Bélanger and R. E. Crossler, "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Q.*, vol. 35, no. 4, pp. 1017–1041, 2011.

[13] D. H. McKnight, L. L. Cummings, and N. L. Chervany, "Initial Trust Formation in New Organizational Relationships," *Acad. Manag. Rev.*, vol. 23, no. 3, pp. 473–490, Jul. 1998.

[14] M. Fishbein and I. Ajzen, *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley, 1975.

[15] G. R. Milne and A. J. Rohm, "Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives," *J. Public Policy Mark.*, vol. 19, no. 2, pp. 238–249, 2000.

[16] A. D. Miyazaki and A. Fernandez, "Internet privacy and security: An examination of online retailer disclosures," *J. Public Policy Mark.*, vol. 19, no. 1, pp. 54–61, 2000.

[17] K. B. Sheehan and M. G. Hoy, "Dimensions of privacy concern among online consumers," *J. Public Policy Mark.*, vol. 19, no. 1, pp. 62–73, 2000.

[18] S. Grazioli and S. L. Jarvenpaa, "Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers," *IEEE Trans. Syst. Manag. Cybern. Part A Syst. Humans*, vol. 30, no. 4, pp. 395–410, 2000.

[19] D. Gefen, E. Karahanna, and D. W. Straub, "Trust and TAM in Online Shopping: An Integrated Model," *MIS Q.*, vol. 27, no. 1, pp. 51–90, 2003.

[20] G. R. Dowling and R. Staelin, "A Model of Perceived Risk and Intended Risk-handling Activity," *J. Consum. Res.*, vol. 21, no. June, pp. 119–134, 1994.

[21] I. Ajzen and M. Fishbein, *Understanding attitudes and predicting social behavior*. Englewood Cliffs: Prentice-Hall, 1980.

[22] S. L. Jarvenpaa, N. Tractinsky, and M. Vitale, "Consumer Trust in an Internet Store," *Inf. Technol. Manag.*, vol. 1, pp. 45–71, 2000.

[23] E. C. Tandoc, P. Ferrucci, and M. Duffy, "Facebook use, envy, and depression among college students: Is facebooking depressing?," *Comput. Human Behav.*, vol. 43, pp. 139–146, 2015.

[24] N. Keresztes, B. Pikó, and M. Fülöp, "Does Competitiveness Count?," *Eur. J. Ment. Heal.*, vol. 10, no. 1, pp. 44–61, 2015.

[25] R. D. Smither and J. M. Houston, “The nature of competitiveness: construction and validation of the Competitiveness Index,” *Educ. Psychol. Meas.*, vol. 52, pp. 407–418, 1992.
[26] J. M. Houston, P. B. Harris, and D. Francis, “Revising the Competitiveness Index,” *Psychol. Rep.*, vol. 90, pp. 31–34, 2002.
[27] P. B. Harris and J. M. Houston, “A reliability analysis of the revised competitiveness index,” *Psychol. Rep.*, vol. 106, no. 3, pp. 870–874, 2010.
[28] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, “Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies,” *J. Appl. Psychol.*, vol. 88, no. 5, pp. 879–903, Oct. 2003.
[29] S. B. Mackenzie, P. M. Podsakoff, and N. P. Podsakoff, “Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques,” *MIS Q.*, vol. 35, no. 2, pp. 293–334, 2011.
[30] G. A. Churchill, “A Paradigm for Developing Better Measures of Marketing Constructs,” *J. Mark. Res.*, vol. 16, no. February, pp. 64–73, 1979.
[31] J. P. Peter, “Construct Validity: A Review of Basic Issues and Marketing Practices,” *J. Mark. Res.*, vol. 18, no. 2, pp. 133–145, 1981.
[32] D. W. Straub, M.-C. Boudreau, and D. Gefen, “Validation Guidelines for IS Positivist Research,” *Commun. AIS*, vol. 13, pp. 381–427, 2004.
[33] C. Fornell and D. F. Larcker, “Evaluating Structural Equation Models with Unobservable Variables and Measurement Error,” *J. Mark. Res.*, vol. 18, pp. 39–50, 1981.
[34] C. M. Ringle, S. Wende, and A. Will, “SmartPLS.” SmartPLS, Hamburg, Germany, 2005.
[35] W. Wang and I. Benbasat, “Trust in and Adoption of Online Recommendation Agents,” *J. Assoc. Inf. Syst.*, vol. 6, no. 3, pp. 72–101, 2005.
[36] H. Liang and Y. Xue, “Understanding Security Behaviors in Personal Computer Usage : A Threat Avoidance Perspective,” *J. Assoc. Inf. Syst.*, vol. 11, no. 7, pp. 394–413, 2010.
[37] F. K. Y. Chan, J. Y. L. Thong, V. Venkatesh, S. A. Brown, P. J. Hu, and K. Y. Tam, “Modeling Citizen Satisfaction with Mandatory Adoption of an E-Government Technology,” *J. Assoc. Inf. Syst.*, vol. 11, no. 10, pp. 519–549, 2010.